МОСКОВСКИЙ КРИМИНОЛОГИЧЕСКИЙ КАБИНЕТ

ЭФФЕКТИВНОСТЬ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ: ПРОБЛЕМНЫЕ ВОПРОСЫ

Болсуновская Л.

Аннотация: *В статье рассматривается проблема противодействия киберпреступности уделялось значительное внимание.Как уже упоминалось, определение границ киберпреступности имеет принципиальное значение. Решая вопрос о круге деяний, относимых к сфере киберпреступлений, прояснится структура киберпреступности. Поскольку на базе МВД создан специальный отдел «К», постольку именно этот отдел должен заниматься делами о киберпреступлениях. Непоследовательная реализация данного подхода в правоохранительной системе приведет на практике к беспорядку и злоупотреблениям со стороны сотрудников правоохраны. Метод или методология исследования: (не менее 15 слов) Применив общенаучные методы анализа и сравнения, проанализирована законодательная конструкция состава хищения предметов, имеющих особую ценность, а также момент окончания данного преступления. Интерес представляет статистический отчет, подготовленный неофициальным субъектом учета, специалистами лаборатории криминалистики международной компании Group-IB за 2011-2014 годы. Так, согласно данным отчета Group-IB, объем рынка киберпреступности в РФ и СНГ составил: в 2011 г. – 2,055 млрд $, в 2012 г. – 1,938 млрд $, в 2013 г. (вторая половина) – 2014 г. (первая половина) – 2,501 млрд $. Составителями отчета киберпреступность, во-первых, понимается в узком смысле слова, а во-вторых, как экономическая модель преступности.*
Ключевые слова: *Эффективность, противодействие, киберпреступность, проблема, вопрос, предупреждение, ликвидация, компьютерные атаки, информационные ресурсы, экономическая модель преступности.*

В рамках Двенадцатого Конгресса ООН по предупреждению преступности и уголовному правосудию (12-19 апреля 2010 г., Салвадор, Бразилия) проблеме противодействия киберпреступности уделялось значительное внимание.

В материалах Конгресса[1] были обозначены два исторических этапа развития киберпреступности.

Первый этап датирован периодом с 1960 по 1980 годы. Характеризуется преступными посягательствами на конфиденциальность, целостность и доступность данных. Второй этап связывают с появлением графического интерфейса для работы с компьютерами и развитием публичной сети – с 1990 года по настоящее время. Для данного периода характерно качественное видоизменение киберпреступности: преступления преимущественно связаны с сетью.

К основным причинам, вызывающим трудности при выработке мер социально-правового контроля, относятся [2]:

– различия в подходах на уровне национального законодательства (круг криминализированных деяний);

DOI: 10.7256/2310-8681.2014.4.15823

– неясность масштабов (отсутствие криминальной статистики по отдельным видам преступлений);

– транснациональный аспект (киберпреступность носит в значительной степени транснациональный характер);

– киберпреступность рассматривается в контексте новой формы организованной преступности.

В документах Десятого Конгресса ООН по предупреждению преступности и обращению с правонарушителями (10-17 апреля 2000 г., Вена) [3] обобщаются подходы к пониманию киберпреступности, которая рассматривается в широком и узком смысле.

В публикации Международного Союза Электросвязи «Понимание киберпреступности: руководство для развивающихся стран»[4], а также в Конвенции Совета Европы о киберпреступности 2001 года [5] (далее по тексту Конвенция) с учетом положений дополнительного Протокола к Конвенции от 2003 года[6] концептуально закрепляется понимание киберпреступности в широком смысле слова. И, соответственно, киберпреступность определяется как совокупность деяний, в которых инструментом, целью или местом преступных действий являются компьютеры или сети.

В национальном правопорядке доминирует подход к пониманию киберпреступности в узком смысле слова. Речь идет о гл. 28 УК РФ – преступления в сфере компьютерной информации, и о составе – мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) [7].

Вопрос об определении границ в описании киберпреступности, тем не менее имеет принципиальное практическое значение.

Во-первых, от круга деяний, относимых к сфере киберпреступлений, зависит и система мер, направленных на снижение уровня киберпреступности.

Во-вторых, станет возможной постановка вопроса об оценке эффективности противодействия киберпреступности.

Анализ официальных статистических данных МВД России за период с 1997 по 2014 годы [8] показывает, что пик регистрируемой компьютерной преступности приходится на 2009 год и составляет 11636 преступлений. По итогам 2014 года по отношению к 2009 году количество зарегистрированных преступлений уменьшилось в 6,7 раз. Но, при этом, по отношению к 1997 году, прирост учтенных преступлений, предусмотренных гл. 28 УК РФ, составил 24843%, то есть увеличение числа регистрируемой компьютерной преступности в 248 раз.

Вызывают вопросы сведения, полученные из доклада начальника Бюро специальных технических мероприятий МВД России А. Н. Мошкова.

На национальном уровне, начиная с 2001 года, на регулярной основе проводится национальный форум информационной безопасности[9]. Так, в рамках 15-го форума глава отдела «К» МВД сообщил[10], что в 2012 году в России зарегистрировано на 28% больше высокотехнологичных преступлений в сравнении с предыдущим годом. Однако, согласно статистике МВД прирост за обозначенный период по гл. 28 УК РФ составил 4,5%. Далее, «наиболее массовыми и прибыльными видами преступлений, совершаемыми с использованием компьютерных и телекоммуникационных технологий, являются мошенничества и кражи денежных средств со счетов граждан и организаций»[11]. Так, в 2012 году подразделением «К» МВД было зарегистрировано 3645 подобных преступлений, а в 2011 году их было 2123, то есть, прирост на 72%. Кроме того, в 2012 году было возбуждено 169 уголовных дел за «изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних, с использованием информационно-телекоммуникационных сетей (включая сеть Интернет)» (п. «г» ч.2 ст. 242.1)[11].

Первое, что обращает на себя внимание – как соотносятся цифры 28% прироста высокотехнологичных преступлений с приростом на 72% компьютерных хищений? Второе, что вкладывается в понятие высокотехнологичные преступления, и как это понятие соотносится с понятием киберпреступность? И какова структура киберпреступности?

Сравним положения Конвенции и дополнительного Протокола с положениями национального уголовного закона. Если применить подход, закрепленный в Конвенции к пониманию киберпреступности в широком смысле слова, нам придется согласиться с тем, что к киберпреступлениям относятся: преступления в сфере компьютерной информации (гл. 28 УК РФ), мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), оборот детской порнографии (п. «г» ч.2 ст. 242.1, п. «г» ч.2 ст. 242.2 УК РФ), нарушение авторских и смежных прав (ст. 146 УК РФ) и преступления ненависти (ст. 282 УК РФ).

Но, согласно Уголовно-процессуальному кодексу России[12] не все обозначенные пре-

DOI: 10.7256/2310-8681.2014.4.15823

ступления подследственны МВД и, в частности, отделу «К».

Так, дела о преступлениях ненависти (ст. 282 УК РФ), использование несовершеннолетнего в целях изготовления порнографических материалов или предметов (ст. 242.2 УК РФ) и нарушение авторских и смежных прав (ст. 146 УК РФ) подследственны Следственному Комитету.

Осложняет ситуацию в оценке эффективности противодействия киберпреступности Указ Президента России от 15 января 2013 года за № 31с (выписка) «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ»[13].

Во исполнение положений Указа Президента ФСБ РФ подготовлен ряд законопроектов[14]. В интересующей нас части изменения направлены на преступления в сфере компьютерной информации. Вводятся особо квалифицированные составы в статью 272 и статью 274 УК РФ «деяния, …, если они повлекли ущерб безопасности критической информационной инфраструктуры Российской Федерации или создали угрозу его наступления»[14]. Названные преступления согласно законопроекту подследственны органам ФСБ РФ. Основная цель законопроекта «О безопасности критической информационной инфраструктуры РФ» заключается в предотвращении компьютерных инцидентов, в том числе вызванных компьютерной атакой. Согласно ст. 2 вышеназванного законопроекта компьютерная атака – целенаправленное воздействие на информационные ресурсы программно-техническими средствами, осуществляемое в целях нарушения безопасности информации в этих ресурсах. Компьютерный инцидент (ст. 2) – факт нарушения (или прекращения) функционирования объекта критической информационной инфраструктуры Российской Федерации, в том числе вызванный компьютерной атакой. Фактически, под компьютерной атакой понимается DDos-атака, если пользоваться международной терминологией, которая определяется как атака, направленная на отказ в обслуживании[15].

Вопрос об установлении уголовной ответственности за DDos–атаки в уголовно-правовой науке поднимался уже давно[16]. И данное решение стоит расценивать положительно. Но проблема заключается в том, что ст. 272 УК РФ предполагает неправомерный доступ к информации. Который, во-первых является несанкционированным обладателем[17] информации, (субъект не имеет право на информацию, доступ к которой он получает), во-вторых, в отношении подобной информации установлен особый режим, режим ограниченного доступа[18]. Особенность атаки, направленной на отказ в обслуживании, состоит в том, что доступ к компьютерной информации в таком деянии правомерный. То есть, субъект преступления воздействует на публичную информацию. И результатом такой атаки является блокирование компьютерной информации, к примеру, Интернет-сайта, или при очень высокой мощности атаки может быть заблокирован доступ ко всем информационным ресурсам, которые находятся на атакуемом сервере. Соответственно, установление особо квалифицированного состава преступления в ст. 272 УК РФ приведет к нарушению принципа законности (ч. 2 ст. 3 УК РФ). В этом случае необходима самостоятельная уголовно-правовая норма, устанавливающая ответственность за компьютерные атаки, направленные на отказ в обслуживании. Но данная проблема может быть решена и иначе, нежели уголовно-правовыми средствами, и решение будет более эффективным с точки зрения минимизации последствий атак. А в ряде государств некоторыми общественными движениями и политическими партиями предлагается легализовать DDos-атаки[19], рассматривая их как акт протеста. Что касается предложения об установлении особо квалифицированного состава в ст. 274 УК РФ, то данное решение не противоречит принципу законности (ч.2 ст. 3 УК РФ).

Интерес представляет статистический отчет, подготовленный неофициальным субъектом учета, специалистами лаборатории криминалистики международной компании Group-IB за 2011-2014 годы [20].

Так, согласно данным отчета Group-IB, объем рынка киберпреступности в РФ и СНГ составил: в 2011 г. – 2,055 млрд $, в 2012 г. – 1,938 млрд $, в 2013 г. (вторая половина) – 2014 г. (первая половина) – 2,501 млрд $.

Исходя из анализа отчета, можно заключить, что составителями отчета киберпреступность, во-первых, понимается в узком смысле слова, а во-вторых, как экономическая модель преступности.

Как уже упоминалось, определение границ киберпреступности имеет принципиальное значение. Решая вопрос о круге деяний, относимых к сфере киберпреступлений, прояснится структура киберпреступности. Поскольку на базе МВД создан специальный отдел «К», постольку

DOI: 10.7256/2310-8681.2014.4.15823

именно этот отдел должен заниматься делами о киберпреступлениях. Непоследовательная реализация данного подхода в правоохранительной системе приведет на практике к беспорядку и злоупотреблениям со стороны сотрудников правоохраны. Безусловно, гл. 28 УК РФ нуждается в реформировании. В качестве ориентира могут выступать положения Конвенции. Поскольку социально-правовой контроль над преступностью включает и предупреждение (профилактику), то, как нам представляется, из конкретных мер, направленных на минимизацию последствий киберпреступности, эффективнее всего будет виктимологическая профилактика. А также комплекс аппаратно-программных, или технических, мер предупреждения киберпреступности.

Библиография:

1. Двенадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию. A/CONF.213/1
2. Десятый Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями. A/CONF.187/1
3. www.itu.int/ITU-D/cyb/cybersecurity/legislation.html (дата обращения: 05.04.2015)
4. http://conventions.coe.int/Treaty/RUS/Treaties/Html/185.htm (дата обращения: 05.04.2015)
5. Дополнительный Протокол к Конвенции Совета Европы о киберпреступности (Страсбург, 28 января 2003 года), доступен в системе СПС «КонсультантПлюс»
6. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 30.03.2015), доступен в системе «КонсультантПлюс»
7. ФКУ «Главный информационно-аналитический центр» МВД РФ «Состояние преступности в России»
8. http://infoforum.ru/about (дата обращения: 05.04.2015)
9. https://mvd.ru/news/item/830615/ (дата обращения: 01.04.2015)
10. Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 N 174-ФЗ (ред. от 08.03.2015) (с изм. и доп., вступ. в силу с 20.03.2015), доступен в системе «КонсультантПлюс»
11. Собрание законодательства РФ, 21.01.2013, N 3, ст. 178
12. Проект ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Проект Федерального закона «О внесении изменений в законодательные акты РФ в связи с принятием ФЗ «О безопасности критической информационной инфраструктуры РФ» (документы доступны в системе «КонсультантПлюс»)
13. Русский рынок компьютерных преступлений. Состояние и тенденции. 2011г. (www.group-ib.ru) (дата обращения: 05.04.2015)
14. Зинина У.В. «Преступления в сфере компьютерной информации в Российском и Зарубежном уголовном праве», канд. дисс. г. Москва, 2007 г. – С. 149 (Хотя автор предлагает ввести уголовную ответственность за Dos – атаки, но это не принципиальная разница)
15. ст. 6 ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (с изм.и доп), доступен в системе «КонсультантПлюс»
16. Степанов-Егиянц В.Г. Объективная сторона неправомерного доступа к компьютерной информации по Уголовному кодексу РФ // Статья, доступна в системе «КонсультантПлюс»
17. Минин А. Я. «Кибербезопасность и защита информационных систем» // Статья (доступна в системе «КонсультантПлюс»)
18. www.group-ib.ru (дата обращения: 05.04.2015)

References (transliterated):

1. Dvenadtsatyi Kongress Organizatsii Ob''edinennykh Natsii po preduprezhdeniyu prestupnosti i ugolovnomu pravosudiyu. A/CONF.213/1
2. Desyatyi Kongress Organizatsii Ob''edinennykh Natsii po preduprezhdeniyu prestupnosti i obrashcheniyu s pravonarushitelyami. A/CONF.187/1
3. www.itu.int/ITU-D/cyb/cybersecurity/legislation.html (data obrashcheniya: 05.04.2015)

DOI: 10.7256/2310-8681.2014.4.15823

4. http://conventions.coe.int/Treaty/RUS/Treaties/Html/185.htm (data obrashcheniya: 05.04.2015)
5. Dopolnitel'nyi Protokol k Konventsii Soveta Evropy o kiberprestupnosti (Strasburg, 28 yanvarya 2003 goda), dostupen v sisteme SPS «Konsul'tantPlyus»
6. Ugolovnyi kodeks Rossiiskoi Federatsii ot 13.06.1996 N 63-FZ (red. ot 30.03.2015), dostupen v sisteme «Konsul'tantPlyus»
7. FKU «Glavnyi informatsionno-analiticheskii tsentr» MVD RF «Sostoyanie prestupnosti v Rossii»
8. http://infoforum.ru/about (data obrashcheniya: 05.04.2015)
9. https://mvd.ru/news/item/830615/ (data obrashcheniya: 01.04.2015)
10. Ugolovno-protsessual'nyi kodeks Rossiiskoi Federatsii" ot 18.12.2001 N 174-FZ (red. ot 08.03.2015) (s izm. i dop., vstup. v silu s 20.03.2015), dostupen v sisteme «Konsul'tantPlyus»
11. Sobranie zakonodatel'stva RF, 21.01.2013, N 3, st. 178
12. Proekt FZ «O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii», Proekt Federal'nogo zakona «O vnesenii izmenenii v zakonodatel'nye akty RF v svyazi s prinyatiem FZ «O bezopasnosti kriticheskoi informatsionnoi infrastruktury RF» (dokumenty dostupny v sisteme «Konsul'tantPlyus»)
13. Russkii rynok komp'yuternykh prestuplenii. Sostoyanie i tendentsii. 2011g. (www.group-ib.ru) (data obrashcheniya: 05.04.2015)
14. Zinina U.V. «Prestupleniya v sfere komp'yuternoi informatsii v Rossiiskom i Zarubezhnom ugolovnom prave», kand. diss. g. Moskva, 2007 g. – S. 149 (Khotya avtor predlagaet vvesti ugolovnuyu otvetstvennost' za Dos – ataki, no eto ne printsipial'naya raznitsa)
15. st. 6 FZ «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii» ot 27.07.2006 № 149-FZ (s izm.i dop), dostupen v sisteme «Konsul'tantPlyus»
16. Stepanov-Egiyants V.G. Ob''ektivnaya storona nepravomernogo dostupa k komp'yuternoi informatsii po Ugolovnomu kodeksu RF // Stat'ya, dostupna v sisteme «Konsul'tantPlyus»
17. Minin A. Ya. «Kiberbezopasnost' i zashchita informatsionnykh sistem» // Stat'ya (dostupna v sisteme «Konsul'tantPlyus»)
18. www.group-ib.ru (data obrashcheniya: 05.04.2015)

DOI: 10.7256/2310-8681.2014.4.15823